Af

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Alan Dowd et al.

Title: NETWORK SECURITY MODELING SYSTEM AND METHOD

Docket No.: 105.176US1
Filed: January 14, 2000
Examiner: Dwin M Craig

Serial No.: 09/483,127
Due Date: October 28, 2006
Group Art Unit: 2123

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

X Return postcard.
X Appeal Brief (36 pgs.).
X Permission to charge Deposit Account No.19-0743 in the amount of $250.00 to cover the Appeal Brief Filing Fee.

Please consider this a PETITION FOR EXTENSION OF TIME for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: Thomas F. Brennan
Atty: Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 25th day of October, 2006.

Amy Moriarty
Name

Signature

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
(GENERAL)

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Alan Dowd et al. Examiner: Dwin M. Craig

Serial No.: 09/483,127 Group Art Unit: 2123

Filed: January 14, 2000 Docket: 105.176US1

For: NETWORK SECURITY MODELING SYSTEM AND METHOD

APPEAL BRIEF UNDER 37 CFR § 41.37

Mail Stop Appeal Brief- Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The Appeal Brief is presented in support of the Notice of Appeal to the Board of Patent Appeals and Interferences, filed on August 24, 2006, from the rejection of claims 1-25, 27-31, 33-36 and 38-42 of the above-identified application, as set forth in the Office Action mailed on May 24, 2006.

The Commissioner of Patents and Trademarks is hereby authorized to charge Deposit Account No. 19-0743 in the amount of 250.00 which represents the requisite fee set forth in 37 C.F.R. § 41.2(b)(2). The Appellants respectfully request consideration and reversal of the Examiner's rejections of pending claims 1-25, 27-31, 33-36 and 38-42.

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, SECURE COMPUTING CORPORATION.

2. RELATED APPEALS AND INTERFERENCES

Appellants know of no other appeals or interferences which will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 1-42 are pending; claims 1-25, 27-31, 33-36 and 38-42 have been rejected, and are the subject of the present appeal.

4. STATUS OF AMENDMENTS

All amendments have been entered. The last amendment was made in the Amendment and Response filed April 21, 2003.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As noted in the Background of the present patent application, the amount of information being transferred between systems internal and external to a network continues to increase, creating a need for improved network security tools. Conventional network vulnerability tools do not look at the interactions between network components or show the path of an attack. These tools may not look at both the internal and external face of the network. Additionally, tools that assess vulnerabilities through controlled attacks on the network leave footprints such as log entries and may disrupt the network.

The present application describes a network security modeling system, a method for assessing network vulnerabilities, a method for opposing network attackers and a game based on such a security modeling system.

Appellant teaches at Fig.1 and p. 4, line 28 through p. 5, line 5, and claims in claim 1, and dependent claims 2-8, a security modeling system having a network configuration module and a simulator coupled to the network configuration module. The simulator includes a network vulnerabilities database used to determine network security issues. The network configuration module includes network configuration data stored in a network configuration database (p. 5, lines 6-9).

Appellant teaches at Fig.9 and p. 19, line 24 through p. 20, line 4, and claims in claim 9, and dependent claims 38 and 39, an interactive computer game having a network configuration module and a simulator coupled to the network configuration module. The simulator includes a network vulnerabilities database used to determine network security issues (Fig.1 and p. 4, line 28 through p. 5, line 5). The network configuration module includes network configuration data stored in a network configuration database (p. 5, lines 6-9). The system may have a plurality of client players such as attackers, defenders, or administrators. (p. 20, lines 1-4). Clients attack the network by sending commands that simulate service functionality, change services or nodes, and exploit vulnerabilities (p. 20, lines 14-15). Clients defend network territory by adjusting the posture of nodes, setting router and firewall filtering policies, and resetting nodes or

services that have been disabled or compromised (p. 20, lines 15-17). The system may be used either for entertainment or as a training tool to educate personnel involved with network security in building and protecting secure networks (p. 20, lines 5-7)

Appellant teaches at Fig. 2 and p. 7, line 28 through p. 9, line 9, and claims in claim 10, and dependent claims 11-17, a security modeling system having a network configuration module, a simulator coupled to the network configuration module and a mission objectives module coupled to the simulator. The simulator includes a network vulnerabilities database used to determine network security issues. The network configuration module includes network configuration data stored in a network configuration database (p. 5, lines 6-9). The mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario (p. 9, line 1-9). The mission objectives module contains critical resource information such as goals, expectations, and constraints for simulating the network (p. 9, lines 1-3). The information may be used to determine that a particular entity is important for a specific attack scenario (p. 9, lines 3-5). Mission objectives data may be contained in a plurality of tables and modeled as components or services that need to be protected against attacks (p. 17, lines 25-32).

In one embodiment, the network configuration database contains a plurality of network tables such as a node table, routing table, configuration table, and filter table (p. 13, line 25 – p. 14, line 1). Network configuration data may be received from an objective network, the output of a network configuration discovery tool, or a system administrator (p. 11, lines 23 – 26). Stored network configuration data can be used to run multiple tests or attack strategies on a single network configuration. In one embodiment, a user is allowed to modify the network configuration data. This allows system administrators to either test the results of adding new components to an existing network or test the design of a non-existent network (p. 9, line 24 – p. 10, line 3). An illustration of one embodiment of the network configuration database is shown in Figure 7.

The network vulnerabilities database contains vulnerability data about conventional network components, hardware and software (p. 5, lines 10 – 12). Specifically, each entry contains the service including version and patch levels, defense

conditions that might close the vulnerability, the resource and state conditions needed to exercise the vulnerability and the effects of exploiting the vulnerability (p. 17, lines 2-7).

Simulations are run to determine network vulnerabilities using vulnerability and network configuration data. The simulator is capable of simulating a variety of networks including enterprise networks, wide area networks and local area networks using the network configuration data (p. 5, lines 1-3). The simulator is also able to simulate network components such as servers, workstations, routers and firewalls, as well as the protocols and services that run on the components (p. 5, lines 3-5). The simulator analyzes interactions between network components, the interior and the exposed face of the network. Simulations can be preformed based on specific attack scenarios using configuration and vulnerability data, general attack scenarios, or attack scenarios determined by a system administrator or other user (p. 6, lines 15-17; p. 7, lines 6-9)

Appellant teaches, and claims in claim 18, and dependent claims 19-27, a method of analyzing computer network security using a modeling system. As shown at p. 2, lines 25-30, Figure 1 and p. 4, line 28 through p. 7, line 26, the method comprises providing a network configuration of a computer network, simulating the network based on the configuration, and determining vulnerabilities of the simulated network using the vulnerability information stored in the database.

As claimed in claim 40, and dependent claims 41 and 42, a method comprising providing a network configuration of a computer network, simulating the network based on the configuration, and determining vulnerabilities of the simulated network using the vulnerability information stored in the database (as shown at p. 2, lines 25-30, Figure 1 and p. 4, line 28 through p. 7, line 26) can be stored on a machine readable medium.

Appellant teaches, and claims in claim 28, and dependent claims 29-33, a method of opposing network attackers. As shown at p. 3, lines 1-6, Figure 3 and p. 11, line 6-22, the method includes receiving a network configuration, receiving mission objectives, receiving commands from a network attacker, simulating the network based on the commands received from the attacker, and responding to the network attacker.

Appellant teaches at Fig. 2 and p. 7, line 28 through p. 9, line 9 and p. 9, line 22 through p. 10, line 19, and claims in claim 34, and dependent claims 35-37, a security

modeling system having a simulator and a graphical user interface. The simulator includes mission objectives tables and network configuration tables having network configuration data. Mission objectives data may be contained in a plurality of tables and modeled as components or services that need to be protected against attacks (p. 17, lines 25-32).

This summary does not provide an exhaustive or exclusive view of the present subject matter, and Appellants refer to the appended claims and its legal equivalents for a complete statement of the invention.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Are claims 1-8 and 18-20 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Lewis (U.S. Patent No. 6,014,697), in view of Shostack (U.S. Patent No. 6,298,445)?

Are claims 10-25, 27-31, 33-36 and 40-42 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Lewis (U.S. Patent No. 6,014,697), in view of Huff (U.S. Patent No. 6,408,391)?

Are claims 9, 38 and 39 properly rejected under 35 USC § 103(a) as being unpatentable over the combination of Lewis (U.S. Patent No. 6,014,697), in view of Huff (U.S. Patent No. 6,408,391), and further in view of Official Notice?

7. ARGUMENT

Official Notice

1) The Applicable Law

As detailed in *Ahlert* and as noted in the M.P.E.P. at 2144.03.E.,

> Any rejection based on assertions that a fact is well-known or is common knowledge in the art without documentary evidence to support the examiner's conclusion should be judiciously applied. Furthermore, as noted by the court in *Ahlert*, any facts so noticed should be of notorious character and serve only to "fill in the gaps" in an insubstantial manner which might exist in the evidentiary showing made by the examiner to support a particular ground for rejection. It is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection was based. See *Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697; *Ahlert*, 424 F.2d at 1092, 165 USPQ 421.

Rejections under U.S.C. § 103

1) The Applicable Law

According to *M.P.E.P.* § 2141, which cites *Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986), the following tenets of patent law must be adhered to when applying 35 U.S.C. § 103. First, the claimed invention must be considered as a whole. Second, the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination. Third, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention. Fourth, obviousness is determined using a reasonable expectation of success standard. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. *M.P.E.P.* § 2141 (citing *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966)).

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or

in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on Appellants' disclosure. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). The references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references. *M.P.E.P.* § 2142 (citing *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)). In considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw there from. *M.P.E.P.* § 2144.01 (citing *In re Preda*, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)). However, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *M.P.E.P.* § 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

In order to take into account the inferences which one skilled in the art would reasonably make, the examiner must ascertain what would have been obvious to one of ordinary skill in the art at the time the invention was made. *M.P.E.P.* § 2141.03 (citing *Environmental Designs, Ltd. v. Union Oil Co*, 713 F.2d 693, 218 USPQ 865 (Fed. Cir. 1983), *cert. denied*, 464 U.S. 1043 (1984)).

> The examiner must step backward in time and into the shoes worn by the hypothetical "person of ordinary skill in the art" when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention "as a whole" would have been obvious at that time to that person. Knowledge of Appellants' disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject

> matter as a whole" of the invention. The tendency to resort to "hindsight" based upon Appellants' disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.

M.P.E.P. § 2141.03.

2) Application of §103 to the Rejected Claims

Claims 1-8 were rejected under 35 USC § 103(a)

Claims 1-8 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Lewis (U.S. Patent No. 6,014,697), in view of Shostack (U.S. Patent No. 6,298,445). Appellant respectfully submits that the Examiner has failed to meet his burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness.

As noted above, in order to establish a *prima facie* case of obviousness, the Examiner must meet three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

Lewis describes a system and method for populating a network simulator tool. Lewis states at col. 1, lines 20-35:

> In order to accurately simulate the behavior of a live network, accurate network topology information must be provided to the network simulation tool. In the prior art, the simulation tools require a user to manually construct a network model. Typically, the user would construct a network model by hand with a special-purpose graphics package.
>
> However, this prior art method is time-consuming and error-prone. In this prior art method, the user must have a conception of the model, or else consult other engineers, before building the model for the simulation tool. Consumption of time and error may result from the conceptualization process and in the manual entering of the network model. A more time-efficient and accurate means for providing topology information of a live network to the network simulator is highly desirable.

Lewis describes a way of automatically discovering the topology and traffic information of a live network and of providing that information to a simulation tool.

The Examiner stated that Lewis describes a system including "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module to simulate and analyze networks based on the network configuration data". The Examiner goes on to say that Lewis does not disclose that the "simulator includes a network vulnerabilities database, and wherein the network vulnerabilities database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability" as described by Applicant and claimed in claims 1-8.

The Examiner stated that Shostack, however, discloses network vulnerability, attack and exploitation data at col.2, line 48 through col. 3, line 37.

Appellant has carefully reviewed Shostack, and in particular the section cited by the Examiner, to find a simulator that "includes a network vulnerabilities database, and wherein the network vulnerabilities database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability" as described by Appellant and claimed in claims 1-8. Shostack does not, however, describe such a simulator. Instead, Shostack describes a network security detector (NSD). The NSD has six components: 1) a database of security vulnerabilities; 2) an application that provides real-time intrusion detection (col. 6, lines 53-65); 3) an application that behaves like a system manager (col. 6, line 66 – col. 7, line 4); 4) an application that simulates attacks on the network and monitors Internet Protocol devices (col. 7, lines 5-19); 5) an application that performs a comprehensive security assessment of the network (col. 7, lines 20-30); and 6) and application that receives software enhancements, including new versions of the software and updates to the database of security vulnerabilities (col. 7, lines 31-35). There is no simulator which simulates and analyzes networks based on network configuration data as described by Appellant and claimed in claims 1-8.

Although Shostack does describe a security vulnerabilities database (Table 1), the security vulnerabilities database is not part of a simulator, connected to a network configuration module, which is used to simulate and analyze networks based on the network configuration data, as described by Appellant and claimed in claims 1-8.

In addition, while Shostack's network vulnerabilities database does include a plurality of known network vulnerabilities, there is no teaching or suggestion in Shostack that each network vulnerability should include a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, as described by Appellant and claimed in claims 1-8.

Finally, as noted above, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. The Examiner stated that it would have been obvious, to one of ordinary skill in the art at the time of the invention, to have used the network vulnerabilities database of Shostack with the network simulation database of Lewis because of the advantages provided by the database of Shostack to prevent damage to a computer network and systems. For support, the Examiner turns to Shostack at col. 2, lines 18-28, which states:

> Whenever an unauthorized user breaches network security and is allowed free access to the system, the damage that might result is unpredictable. However, because some of the system vulnerabilities and techniques used by hackers are known, a system administrator may use that information to make the network less vulnerable to attack. However, the system administrator is required to remain constantly vigilant as to the new attacks being used by hackers, and then use that information to protect the network, clients and servers from the newly found vulnerability.

Appellant respectfully submits that the above passage is simply a statement of a problem that is purportedly solved by Shostack. It is not a suggestion or motivation to combine a reference that can determine network topology (Lewis) with a security suite for testing existing networks (Shostack) to form a security modeling system that uses network configuration data and a security vulnerabilities database to simulate and analyze networks within a network simulator as described by Appellant and claimed in claims 1-

8. Appellant respectfully requests that the Examiner's rejection of claims 1-8 be reversed.

Claims 18-20 were rejected under 35 USC § 103(a)

The Examiner rejected claim 18 based on his analysis of claim 1.

Claim 18 requires that one analyze a computer network using a security modeling system that simulates the network based on a network configuration provided to the security modeling system and that determines vulnerabilities of the simulated network using vulnerability information stored in a database within the security modeling system.

As noted above, neither Lewis nor Shostack, alone or in combination, teach or suggest a security modeling system that simulates the network based on a network configuration and that determines vulnerabilities of the simulated network using vulnerability information stored in a database within the security modeling system as described by Appellant and claimed in claims 18-27. Appellant respectfully requests that the Examiner's rejection of claims 18-27 be reversed.

Furthermore, Appellant respectfully submits that there is no suggestion or motivation in the cited references or in any other source of which Appellant is aware to combine a reference that can determine network topology (Lewis) with a security suite for testing existing networks (Shostack) to form a method of analyzing a computer network using a security modeling system having a security vulnerabilities database which determines vulnerabilities within the simulated network as a function of the vulnerability information stored in the security vulnerabilities database as described by Appellant and claimed in claims 18-27. Appellant respectfully requests that the Examiner's rejection of claims 18-27 be reversed.

Claims 10-25, 27-31, 33-36 and 40-42 were rejected under 35 USC § 103(a)

Claims 10-25, 27-31, 33-36 and 40-42 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Lewis (U.S. Patent No. 6,014,697), in view of Huff (U.S. Patent No. 6,408,391).

The Examiner stated that Lewis describes a system including "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration data."

The Examiner goes on to say that Lewis does not disclose a mission objectives module, with critical resource information and specific attack scenarios but that Huff discloses a mission objectives module, with critical resource information and specific attack scenarios.

The Examiner failed to show where either Lewis or Huff teach "wherein the simulator includes a network vulnerabilities database" as required by claims 10-17. Appellant respectfully requests that the Examiner's rejection of claims 10-17 be reversed.

Even if one was to ignore the requirement "wherein the simulator includes a network vulnerabilities database" as described by Appellant and claimed in claims 10-17, the combination of Lewis and Huff fails to teach every remaining limitation of claims 10-17.

Lewis is discussed above.

Huff describes a security computer system capable of deploying and monitoring software agents on one or more nodes of a network of computers. One type of agent, the "security operative," resides on a node and communicates across the network with a network security server 114. Examples of security operatives are shown as 320, 322, and 324 in Fig. 3. "Each security operative includes a communication framework 410 and an agent core framework 420 and at least one mission, each of which is a software module." Col. 8, lines 35-38.

> As depicted in FIG. 3, the security operatives 320, 322, 324 each include missions such as an audit and intrusion detection mission 452, a change audit mission 454, and a chase mission 456, which are discussed in detail below. Like the communication framework 410, these missions preferably are Java agents. To configure a mission at a communication framework 410, the service request processor module 290 sends a reconfiguration segment to a particular node on the network where the mission is to be deployed. The reconfiguration segment is then instantiated as the mission under instructions from the service request processor module 290.

Col. 9, lines 6-17.

Furthermore,

> The agent core framework 420 includes code necessary for each of the missions to run on a respective node 104, 108, 112 and locally manages each of the missions. The agent core network 420 can receive new missions from the service request processor module 290 and instantiate the new mission on that node based on instructions received from the service request processor module 290. Instantiation is the reserving of memory space and the initializing of the new mission. Under instruction from the service request processor module 290 the agent core framework 420 can receive a mission from another node, can shut off missions on that node, and delete missions if necessary on that node.

Col. 10, lines 3-14.

The Examiner points to Figure 3, references 320, 322 and 324, and numerous places in the text of Huff (including those cited above) for support of his assertion that Huff discloses a mission objectives module, with critical resource information and specific attack scenarios.

As noted above, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). That is, it is insufficient that the Examiner shows a reference that shows software modules with missions. The Examiner must provide a reference (or references) which teach or suggest the entire claim limitation: "a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario." Appellant respectfully submits that the Examiner has failed to do so.

Appellant illustrates a mission objectives module in Figs. 2 and 7 and describes his mission objectives module at p. 9, lines 1-9.

> The mission objectives module 207 which is coupled to the simulator 201 includes critical resource information such as goals, expectations and constraints for simulating the network. The simulator 201 uses the critical resource information to determine that a particular file or other entity such as a service or node, etc., is significant for a specific

> attack scenario or simulation. The information is referred to as mission objectives information and an objectives specification interchangeably. In one embodiment, the mission objectives information is stored in database tables such as mission tables, mission file tables, mission service tables and the like. The data is presented in the tables so as to be processable by a machine such as a computer or microprocessor.

As noted at p. 17, lines 29-32 and illustrated in Fig. 7, "Mission objectives are modeled in the mission tables 780, 782 and 784. Mission objectives are modeled as nodes, files or services that need to be protected against availability, confidentiality and integrity attacks and the like."

And, as noted at p. 20, line 29 through p. 21, line 4,

> A commander will be able to upgrade security measures during different threat scenarios by updating the mission objectives information in order to protect critical resources. For example, during a low threat scenario a commander may determine that information about supplies is not critical but in a higher threat scenario can modify the mission objectives information to identify supply information as a critical resource.

That is, in appellant's approach, the mission objective module is used to drive the simulation by establishing the parameters of the simulation.

In contrast, the "missions" of Huff are software modules that execute on computers within the network to perform functions such as intrusion detection, change audits, or chase missions. There is no "mission objectives module coupled to the simulator" as required by claims 10-17. Furthermore, there is no "mission objectives module.... wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario" as the phrase is used by Applicant in claims 10-17. For these reasons as well, Appellant respectfully requests that the Examiner's rejection of claims 10-17 be reversed.

The Examiner used the combination of Lewis and Huff to reject claims 18-25, 27-31, 33-36 and 40-42 based on the reasoning involved in his rejection of claim 10 above.

As noted above in the discussion of the rejections of claims 10-17, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

Appellant respectfully submits that the Examiner has failed to do so. Each of claims 18-25, 27-31, 33-36 and 40-42 require that the use of a database of network vulnerability information. As the Examiner noted in his rejection of claims 1 and 18 above, Lewis provides no such teaching. Appellant respectfully submits that Huff fails to do so as well.

In addition, Applicant describes and claims in claims 18-27 and 40-42,

> determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes:
>
> a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

As the Examiner noted in his rejection of claims 1 and 18 above, Lewis provides no such teaching. Appellant respectfully submits that Huff fails to do so as well. Appellant respectfully requests that the Examiner's rejection of claims 18-25, 27 and 40-42 be reversed.

Applicant describes, and claims in claims 28-33,

> simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components;

As the Examiner stated in his rejection of claims 1 and 18 above, Lewis does not disclose that the "simulator includes a network vulnerabilities database." It cannot, therefore, simulate "the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components" as described by Appellant and claimed in claims 28-33.

Huff does not teach simulating a network on a simulator, or changing the simulation based on "the network configuration, mission objectives and stored vulnerability data" as described by Appellant and claimed in claims 28-33. As noted above, Huff does not even teach mission objectives, as that term is used by Appellant in the specification and in claims 28-33.

Appellant respectfully requests that the Examiner's rejection of claims 28-31 and 33 be reversed.

Applicant describes, and claims in claims 34-37, a security modeling system comprising:

> a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data;

As the Examiner stated in his rejection of claims 1 and 18 above, Lewis does not disclose that the "simulator includes a network vulnerabilities database." It cannot, therefore, teach or suggest a security modeling system comprising "a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data" as described by Appellant and claimed in claims 34-37.

Huff does not teach simulating a network on a simulator having a plurality of database as described by Appellant and claimed in claims 34-37. As noted above, Huff does not even teach mission objectives, as that term is used by Appellant in the specification and in claims 34-37.

Appellant respectfully requests that the Examiner's rejection of claims 34-37 be reversed.

Claims 9, 38 and 39 were rejected under 35 USC § 103(a)

Claims 9, 38 and 39 were rejected under 35 USC § 103(a) as being unpatentable over the combination of Lewis (U.S. Patent No. 6,014,697), in view of Huff (U.S. Patent No. 6,408,391), and further in view of Official Notice.

Claims 9, 38 and 39 are to a computer game that includes "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game."

The Examiner stated that Lewis describes "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration data.

The Examiner goes on to say that Lewis does not disclose "the database having network vulnerabilities" but that Huff discloses "a database having network vulnerabilities." In addition, the Examiner stated that Huff discloses an interactive GUI.

Finally, the Examiner took Official Notice that real time simulation games are well known in the art and, therefore, that it would have been obvious, to one of ordinary skill in the art at the time the computer game was invented, to provide a computer game that includes "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game" as described by Appellant and claimed in claims 9, 38 and 39.

Lewis and Huff are discussed above.

As noted above in the discussion of the rejections of claims 10-25, 27-31, 33-36 and 40-42, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). Appellant respectfully submits that the Examiner has failed to do so. Each of claims 18-25, 27-31, 33-36 and 40-42 require the use of a database of

network vulnerability information. As the Examiner noted in his rejection of claims 1 and 18 above, Lewis provides no such teaching. Appellant respectfully submits that Huff fails to do so as well.

The Examiner points to DB historical support module 300 in Huff for a teaching of a network vulnerabilities database. Huff states "DB historical support module 300 provides a database of historical information regarding previous threats and misuses and is used by the response engine module 272 in formulating responses." Col. 7, lines 52-55. At col. 7, lines 41-45, Huff states that "Response engine module 272 provides functionality for determining the response that the suppression and countermeasure system should take in response to a threat from an intruder or misuser." At col. 8, lines 52-56, Huff states "A response correlator 412 can provide some of the functionality of the response engine module 272. Advantageously, the response correlator 412 can sometimes eliminate the need for the remote agents 452-458 to communicate with the response engine." At col. 10, lines 54-60, Huff states that

> The response engine module 272 analyzes collected and stored data, detects and characterizes intrusions and misuses, searches a countermeasure database which is stored in the audit database storage unit 286, instructs the service request processor module 290 to dispatch countermeasure agents, monitors for intrusions and misuses, and profiles user data and stores the same in the audit database storage unit 286.

Finally, at col. 11, lines 47-51, Huff states, "When the response engine module 272 detects a suspected intrusion or misuse or an actual intrusion or misuse, then the response engine module 272 alerts the service request processor module 290, which request the agent factory module 296 dispatch an additional mission."

Appellant respectfully submits that Huff is not clear on what is or is not in DB historical support module 300. It appears that DB historical support module 300 may be a historical record of suspected intrusion or misuse incidents, and not a database of vulnerability information as described and claimed by Appellant. This view is buttressed by the statement that "response engine module 272 analyzes collected and stored data, detects and characterizes intrusions and misuses, searches a countermeasure database which is stored in the audit database storage unit 286... [and] instructs the service request

processor module 290 to dispatch countermeasure agents." The countermeasure agents in Huff are predefined software modules dispatched for known vulnerabilities. It would make sense that the data being analyzed is based on events and not vulnerabilities.

In addition, even if Huff could be construed to include a network vulnerabilities database, Huff does not teach or suggest a simulator "wherein the simulator includes a network vulnerabilities database" as described by Applicant and claimed in claims 9, 38 and 39. Appellant respectfully requests that the Examiner's rejection of claims 9, 38 and 39 be reversed.

Furthermore, Appellant respectfully submits that there is no suggestion or motivation to combine a reference that can determine network topology (Lewis) with a security computer system for existing networks (Huff) to form a computer game which simulates attacks on a computer network based on a simulator which uses a network configuration and a network vulnerabilities database as described by Appellant and claimed in claims 9, 38 and 39.

Likewise, there is no teaching or suggestion in either Lewis or Huff to include "a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario" as described by Appellant and claimed in claim 39.

Appellant respectfully requests that the Examiner's rejection of claims 9, 38 and 39 be reversed.

Incorrect Use of Official Notice

As noted above, as detailed in *Ahlert* and as noted in the M.P.E.P. at 2144.03.E., "It is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection was based." See *Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697; *Ahlert*, 424 F.2d at 1092, 165 USPQ 421.

The Examiner stated that real time simulation games are well known in the art and, therefore, that it would have been obvious, to one of ordinary skill in the art at the time the computer game was invented, to provide a computer game that includes "a network configuration module having network configuration data" and "a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game" as described by Appellant and claimed in claims 9, 38 and 39.

Here, the Examiner rejected an independent claim based on an assertion that a fact is well-known or is common knowledge in the art without documentary evidence to support the examiner's conclusion. As noted above, "it is never appropriate to rely solely on common knowledge in the art without evidentiary support in the record as the principal evidence upon which a rejection was based."

Appellant respectfully requests that the Examiner's rejection of claims 9, 38 and 39 be reversed.

It is respectfully submitted that the cited art neither anticipates nor renders the claimed invention obvious and that therefore the claimed invention does patentably distinguish over the cited art. It is respectfully submitted that claims 1-42 should therefore be allowed. Reversal of the Examiner's rejections of claims 1-42 is respectfully requested.

Respectfully submitted,

ALAN DOWD et al.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402

Date October 25, 2006 By Thomas F. Brennan
Thomas F. Brennan
Reg. No. 35,075

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Appeal Brief, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 25th day of October, 2006.

Amy Moriarty
Name

Signature

CLAIMS APPENDIX

1. (Rejected) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module to simulate and analyze networks based on the network configuration data, wherein the simulator includes a network vulnerabilities database, and wherein the network vulnerabilities database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

2. (Rejected) The system of claim 1, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

3. (Rejected) The system of claim 2, wherein the network configuration data and the network vulnerability, attack and exploitation data are stored in database tables and the data is processable by a computer.

4. (Rejected) The system of claim 1, wherein the network configuration module comprises network configuration data output by a network configuration discovery tool.

5. (Rejected) The system of claim 1, wherein the simulator includes a graphical user interface.

6. (Rejected) The system of claim 2, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

7. (Rejected) The system of claim 1, wherein the simulator includes a defender and an attacker user interface.

8. (Rejected) The system of claim 1, wherein the security modeling system is portable.

9. (Rejected) A computer game comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database, and wherein the simulator includes a graphical user interface for playing the game.

10. (Rejected) A security modeling system comprising:

a network configuration module having network configuration data;

a simulator coupled to the network configuration module for simulating and analyzing networks based on the network configuration, wherein the simulator includes a network vulnerabilities database; and

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

11. (Rejected) The system of claim 10, wherein the network vulnerabilities database includes network vulnerability, attack and exploitation data.

12. (Rejected) The system of claim 11, wherein the network configuration data and the network vulnerability, attack and exploitation data is stored in database tables and the data is processable by a computer.

13. (Rejected) The system of claim 10, wherein the simulator includes a graphical user interface.

14. (Rejected) The system of claim 10, wherein the critical resource information includes goals, expectations and constraints for simulating the network.

15. (Rejected) The system of claim 10, wherein the simulator includes a means for receiving the network vulnerability, attack and exploitation data.

16. (Rejected) The system of claim 10, wherein the security modeling system is portable.

17. (Rejected) The system of claim 10, wherein the simulator includes a defender and an attacker interface.

18. (Rejected) A method of analyzing a computer network using a security modeling system, wherein the security modeling system includes a database of network vulnerability information, the method comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes a plurality of known network vulnerabilities, wherein each network vulnerability includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

19. (Rejected) The method of claim 18, wherein providing a network configuration includes receiving a configuration as the output of a network discovery tool.

20. (Rejected) The method of claim 18, wherein providing a network configuration includes receiving a data file which includes a configuration of the computer network.

21. (Rejected) The method of claim 18, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

22. (Rejected) The method of claim 21, wherein determining vulnerabilities includes modifying the simulation using a graphical user interface.

23. (Rejected) The method of claim 22, wherein modifying the simulation includes dynamically interacting with an attacker.

24. (Rejected) The method of claim 22, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

25. (Rejected) The method of claim 23, wherein modifying the simulation includes dynamically interacting in real time with the security modeling system.

26. (Rejected) The method of claim 21, wherein determining vulnerabilities includes computing security results, wherein the security results include a security score.

27. (Rejected) The method of claim 21, wherein determining vulnerabilities of the simulated network includes updating the vulnerabilities database when vulnerabilities are detected.

28. (Rejected) A method of opposing network attackers comprising:

receiving a network configuration, wherein the network configuration comprises computer hardware and software component information;

receiving mission objectives including critical resource information used to determine network components that are involved in a specific attack scenario;

receiving commands from a network attacker;

simulating the network based on the commands received from the network attacker, wherein simulating the network includes determining results as a function of the network configuration, mission objectives and stored vulnerability data for the described computer hardware and software components; and

responding to the network attacker, wherein responding to the attacker includes imposing barriers, providing response messages and protecting the network.

29. (Rejected) The method of claim 28, wherein simulating the network further includes receiving commands from a defender and determining results based on the defender commands.

30. (Rejected) The method of claim 28, wherein receiving configuration includes receiving critical resource information, wherein the critical resource information includes goals, expectation and constraints for simulating the network.

31. (Rejected) The method of claim 28, and further includes modifying the simulation using a graphical user interface.

32. (Rejected) The method of claim 31, wherein determining vulnerabilities includes computing security results which include a security score.

33. (Rejected) The method of claim 31, wherein receiving commands includes receiving attack actions which include commands that simulate service functionality, commands that change services or nodes, and commands that exploit vulnerabilities.

34. (Rejected) A security modeling system for simulating objective networks comprising:

a simulator having a plurality of databases, wherein the plurality of databases include mission objectives tables including information used to determine network components that are involved in a specific attack scenario, vulnerability tables, and network configuration tables, wherein the network configuration tables include network configuration data; and

a graphical user interface which operates with the simulator to allow input and output to clients.

35. (Rejected) The system of claim 34, wherein the mission objectives tables include mission tables, mission files tables and mission services tables.

36. (Rejected) The system of claim 34, wherein the vulnerability tables include service tables.

37. (Rejected) The system of claim 34, wherein the network configuration tables include configuration tables, defense tables, filter tables, node tables, routing tables and password tables.

38. (Rejected) The computer game of claim 9, wherein the simulator further comprises:

an attacker interface to transmit real-time network status information to an attacker during a simulation; and

a defender interface to transmit real-time network status information to a defender during a simulation.

39. (Rejected) The computer game of claim 9 further comprising:

a mission objectives module coupled to the simulator, wherein the mission objectives module includes critical resource information used to determine network components that are involved in a specific attack scenario.

40. (Rejected) A machine-readable medium that provides instructions, which when executed by a machine, cause said machine to perform operations comprising:

providing a network configuration of a computer network;

simulating the network based on the network configuration; and

determining vulnerabilities of the simulated network using the vulnerability information stored in the database, wherein the database includes:

a plurality of known network vulnerabilities, wherein each network vulnerability includes the service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability.

41. (Rejected) The machine-readable medium of claim 40, wherein simulating the network includes:

receiving mission objectives;

storing the objectives; and

simulating the network based on the network configuration and mission objectives.

42. (Rejected) The machine-readable medium of claim 41, wherein mission objectives include critical resource information used to determine network components that are involved in a specific attack scenario.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.